Identidade Digital Autossoberana

Conceitos e iniciativas

Fernando Marino, Blockchain Technical Leader, CPQD

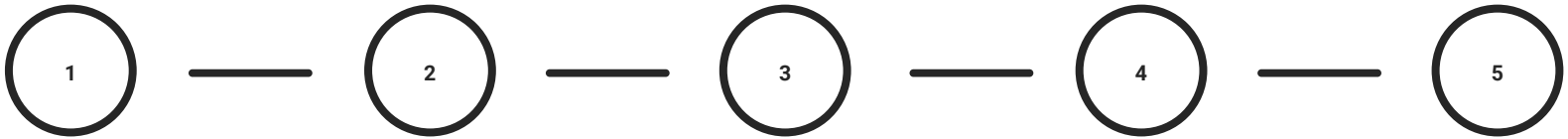
HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

Fernando Marino

***CPQD* - Blockchain Technical Leader**

Pesquisador no CPqD desde 2014, participando de diversos projetos de pesquisa e desenvolvimento de produtos na área de Ciências da Computação, como: mobilidade; visão computacional; IHC (Interação Humano Computador); sistemas acessíveis e mais recentemente Blockchain. Bacharel em Sistemas de Informação pela universidade DeVry Metrocamp em 2014. Atualmente cursa matérias como aluno especial no programa de pós-graduação da Unicamp (Universidade Estadual de Campinas).

Agenda



ID

Contexto da Identidade Digital

SSID

Identidade Digital Autossoberana

Iniciativas

Overview das principais iniciativas globais

Sovrin

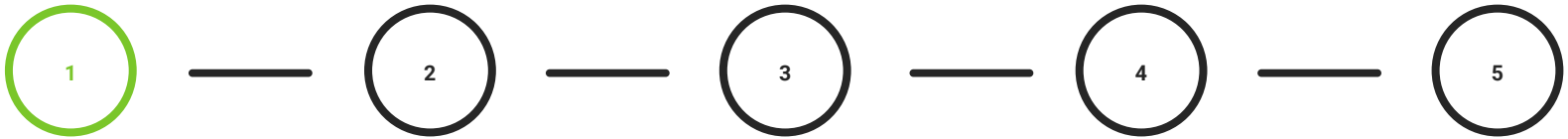
Exemplo de uma plataforma que faz uso do framework Hyperledger Indy

Finalização

Comentários finais

Agenda

Contexto da Identidade Digital



ID

Contexto da Identidade Digital

SSID

Identidade Digital Autossoberana

Iniciativas

Overview das principais iniciativas globais

Sovrin

Exemplo de uma plataforma que faz uso do framework Hyperledger Indy

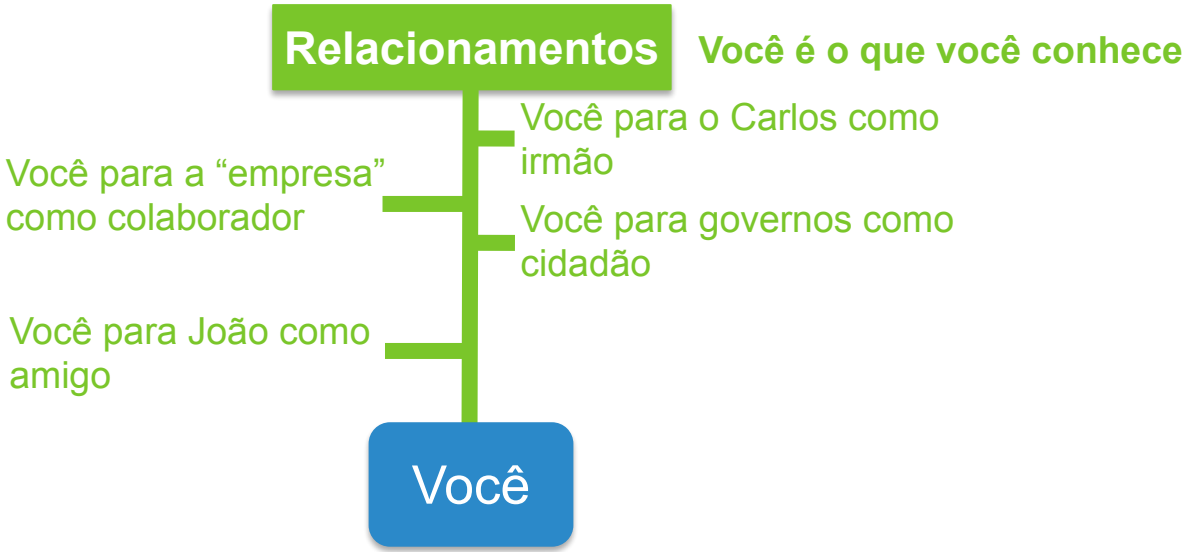
Finalização

Comentários finais

O que é identidade

Aspectos da identidade

Aspectos da identidade



Aspectos da identidade

Aspectos da identidade

Atributos

Relacionamentos

Agentes

Aspectos da identidade

- A identidade digital é a representação digital dos dados relacionados com uma pessoa, empresa, sistema, máquina, acessível através de dispositivos computacionais.

- A identidade digital pode incluir dados biográficos ou biométricos.

Identidade: Mundo físico x digital

No mundo físico: sujeito a ser identificados abre a carteira e mostra a credencial que foi emitida por uma autoridade confiável correspondente.

Qual é o seu equivalente digital para o passaporte, carteira de motorista ou RG? Como usá-los para acessar serviços Web?

E como as credenciais são verificadas?

- No mundo físico, um ser humano faz um julgamento sobre o documento físico.
- No mundo digital, quem faz o julgamento é uma máquina (ou algoritmo).

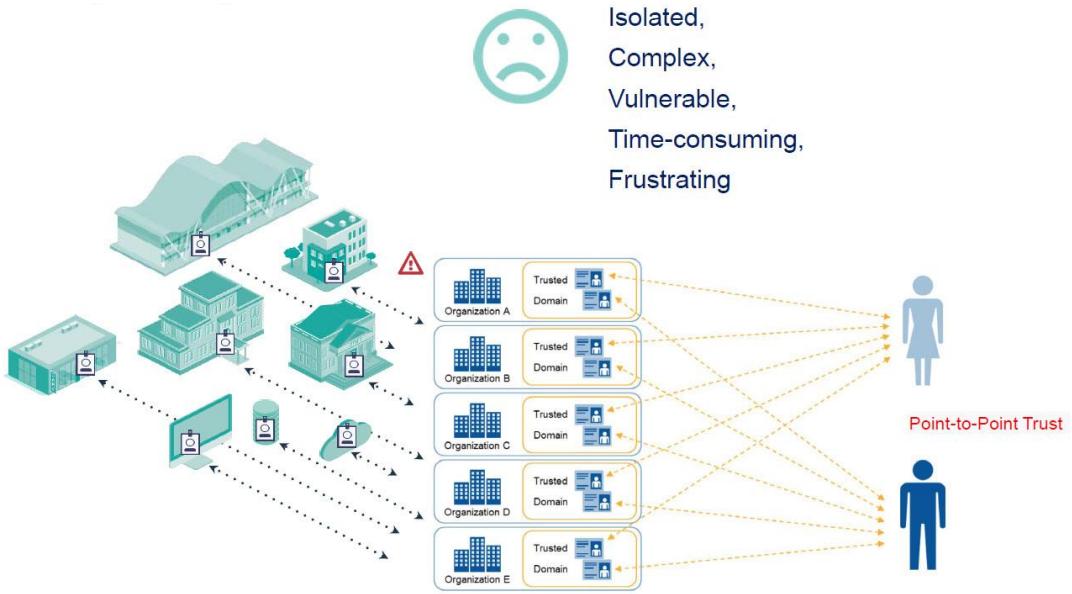
Necessidade para o mundo digital:

- A credencial digital deve ser lida por máquinas, de uma forma padronizada.
- Verificar a origem e a integridade da credencial digital, de uma forma padronizada.

Identidade: Mundo físico x digital

Conceito de identidade no mundo físico é baseado em três componentes:

- Claims: quem ou o que quer que a pessoa esteja reivindicando ser ou ter.
- Provas: documento fornecendo evidências para a reivindicação.
- Atestado: terceiro valida se a reivindicação está correta de acordo com o registro.



Identidade centralizada

- Você nunca possui sua identidade - os sites e aplicativos que a possui.
- Alta probabilidade de fraude e invasão de privacidade.
- Identidade é gerenciada em silos.
- Nomes de usuário e senhas estão espalhados em centenas de sites e aplicativos, juntamente com informações pessoais!
- Abuso de senhas fracas e violações de dados - roubo de informações de identidade são cada vez mais comuns.
- Empresas centralizadas que gerenciam identidade digital têm uma enorme quantidade de dados de usuários e são os principais alvos de ataques - os custos de proteção aumentam a cada dia que passa.

Agenda

Identidade Digital Autossoberana

1

ID

Contexto da Identidade Digital

2

SSID

Identidade Digital Autossoberana

3

Iniciativas

Overview das principais iniciativas globais

4

Sovrin

Exemplo de uma plataforma que faz uso do framework Hyperledger Indy

5

Finalização

Comentários finais

Conceitos: evolução da identidade digital

Modelo de identidade digital
Centralizada e federada

Identidade autossoberana

Conceitos: evolução da identidade digital

Centralizada

- Controlada por uma única entidade, como um site de comércio eletrônico ou uma rede social.

Centralizada

- Na sua forma mais simples, a federação dá um grau de portabilidade a uma identidade centralizada,
- Permite que um usuário faça o login em um serviço usando as credenciais de outro serviço.
- Em um nível mais complexo, permite que diferentes serviços compartilhem detalhes sobre o usuário.

Conceitos: evolução da identidade digital

Centralizada no usuário

- Normalmente estabelecida pela utilização de dispositivos pessoais de autenticação (PAD) ou SSO virtuais.
- Usuário só precisa memorizar uma única senha (do PAD) para vários serviços.

Autossoberana

- É o passo final nessa evolução.
- É independente de qualquer silo.
- Fornece todos os três elementos necessários: controle individual, segurança e total portabilidade.
- Remove os aspectos de controle externo e centralizado das três fases anteriores.

Princípios da SSI

- Existência
- Controle
- Acesso
- Transparência
- Persistência
- Portabilidade
- Interoperabilidade
- Consentimento
- Minimização
- Proteção

Identidade Digital Autossoberana

- Identidade portátil vitalícia para qualquer pessoa, organização ou coisa que não dependa de qualquer autoridade centralizada e que não possa ser eliminada.

- Uma identidade permanente que só pode ser acessada integralmente pela pessoa ou entidade a quem pertence, mas partes dessa identidade podem ser mostradas a qualquer indivíduo, organização ou agência sempre que torna-se relevante e permitido pelo dono da identidade.

- Uma vez que as identidades autossoberanas são descentralizadas, criptografadas e ficam em poder do usuário, o roubo de identidade ou incidentes como o Equifax, Uber, Netshoes, Facebook, Colection #1, #2 e #3 entre outros, se tornam menos problemáticos.

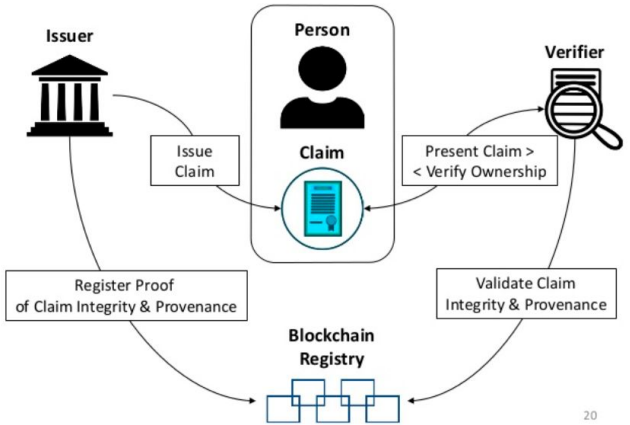
Identidade Autossoberana: características

- Descentralizado, não existe autoridade central
- Baseado na tecnologia blockchain
- Centrada no usuário: ele define como e onde os dados serão utilizados
- Elevados níveis de segurança e privacidade.
- Compatíveis com GDPR e LGDP (não coloca dados pessoais na ledger)
- Portável para diferentes contextos (Bring your own Identity)
- Baixo custo de manutenção
- É considerada a camada de identidade da internet que não foi projetada na sua origem

"On the Internet, nobody knows you're a dog."

Caso de uso ID: SSI e Blockchain

- “Pessoa” é quem detém as informações e os certificados verificáveis.
- Possibilidade de divulgação seletiva de informações e de reivindicações com o consentimento da “Pessoa”.
- Pluralismo de operadores e tecnologias.
- Suporte para apresentação de reivindicações on-line e off-line.
- Métodos de revogação não baseados em CRL-Certificate Revogation List) que elimina a dependência do emissor.
- Alta resistência à exclusão, modificação, mascaramento ou adulteração de dados.



Fonte: https://www.dhs.gov/science-and-technology

Caso de uso ID: SSI e Blockchain

Permite que os indivíduos possuam e controlem a identidade digital: reputação, dados e ativos digitais

Desafios atuais

- KYC / AML (know your customer / anti money laudering) processos caros e demorados
- Controle limitado sobre vazamento de dados
- Depende da confiança em terceiros
- Alta responsabilidade para proteger os dados do usuário
- Ponto único de falha

Benefícios

- Os indivíduos possuem e controlam dados pessoais
- Verificados por várias partes
- As partes não possuem dados confidenciais
- Capacidade de melhorar a conformidade, a resiliência e a interoperabilidade

Agenda

Iniciativas Globais

1

ID

Contexto da Identidade Digital

2

SSID

Identidade Digital Autossoberana

3

Iniciativas

Overview das principais iniciativas globais

4

Sovrin

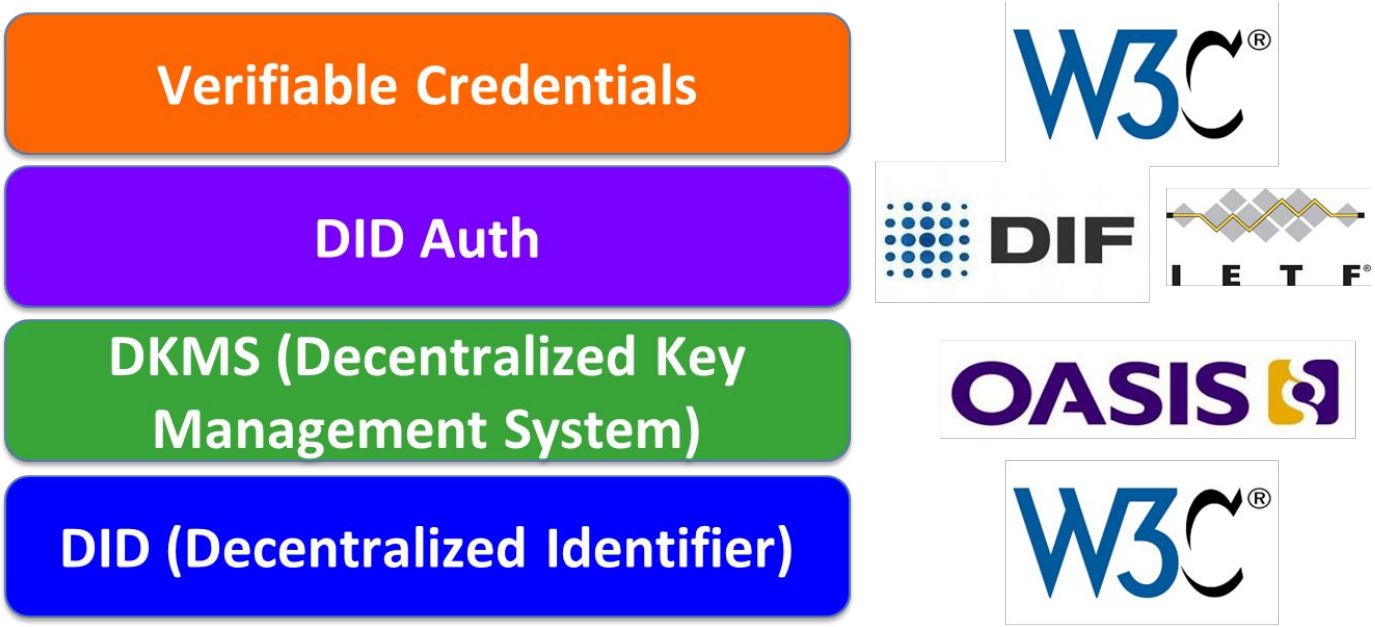
Exemplo de uma plataforma que faz uso do framework Hyperledger Indy

5

Finalização

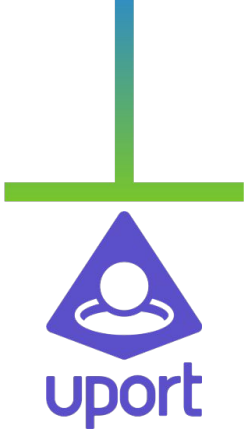
Comentários finais

Identidade Digital Autossoberana: padronização



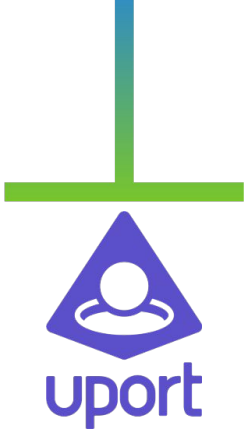
Iniciativas em Identidade Digital

Iniciativas em Identidade Digital: uPort



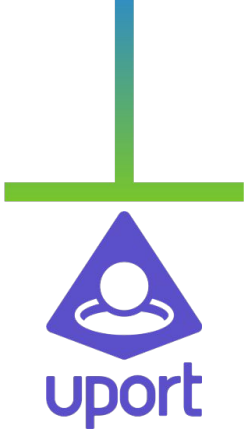
Iniciativas em Identidade Digital: uPort 1/3

- Solução de identidade autossoberana baseada na Ethereum com apoio da Microsoft.
- A tecnologia consiste de contratos inteligentes, bibliotecas de desenvolvimento e aplicação móvel.



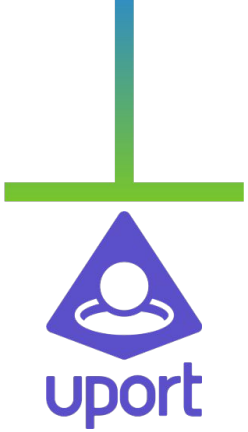
Iniciativas em Identidade Digital: uPort 2/3

- Estão propondo o desenvolvimento de padrões de identidade sobre a Ethereum, mais especificamente, protocolos de verificação para smart contracts. A iniciativa foi bem recebida pela comunidade, porém existe um longo caminho para aplicações em larga escala.
- Na implementação atual, isso é possível com o aplicativo móvel atuando como o principal contêiner seguro para dados relacionados à sua identidade e para um conjunto de chaves que permitem assinar transações, conceder autorização e assinar credenciais.



Iniciativas em Identidade Digital: uPort 3/3

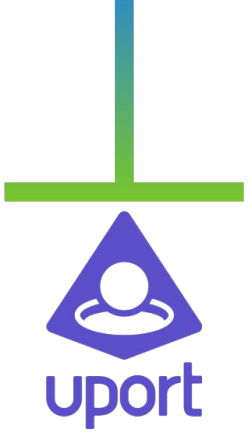
- A identidade é ancorada no blockchain com um identificador e os dados públicos são armazenados no IPFS.



Casos de uso

Self-Sovereign Wallet

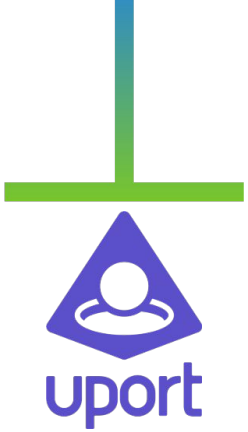
Assine transações e gerencie suas chaves
e dados em um local simples e seguro.



Casos de uso

Credentials

Emita credenciais ou crachás para seus usuários, solicite dados emitidos por outros aplicativos.



Casos de uso

Zug Stadt

Oficialmente a primeira cidade a registrar os cidadãos na rede Ethereum.

Iniciativas em Identidade Digital: Gravity

GRAVITY

1.5 billion people without an official ID

4 billion people without an address

6 billion people with a mobile phone by 2020

Iniciativas em Identidade Digital: Gravity

- Permitir que qualquer pessoa crie um ID digital seguro e autônomo baseado em dados pessoais.
- Utiliza qualquer modelo de telefone celular e independente de operadora.
- Permite que as populações da “Base da Pirâmide” tenham gestão dos dados de identidade.

Casos de uso

Carteiras Digitais

para refugiados, populações apátridas e pessoas deslocadas à força.

Casos de uso

KYC Como um Serviço

para um registo do cartão SIM sem problemas, seguro e barato

Casos de uso

Ajuda Humanitária

melhorar a eficácia da ajuda, garantindo a sua entrega aos beneficiários pretendidos

Iniciativas em Identidade Digital: Sovrin

- Origem do Sovrin: Evernym, em 2015.
- Sovrin Foundation lançada em Setembro de 2016.
- Hoje é uma fundação sem fins lucrativos e um Technical Governance Board.
- Em 2017 a Sovrin Foundation transferiu o código open-source para a Linux Foundation a qual foi a origem do Hyperledger Indy.
- Depois de um ano de sandbox e testes, a Sovrin Network foi fundada em Julho de 2017, com a 1ª transação genesis entre os 10 primeiros participantes, os “stewards”.

Casos de uso

iRespond

usando a Sovrin para fornecer às ONGs sistemas confiáveis de identidade digital

Casos de uso

CULedger

Sovrin para tornar a SSI uma realidade para o Credit Unions

Agenda

Exemplo de Plataforma: Sovrin

ID

Contexto da Identidade Digital

SSID

Identidade Digital Autossoberana

Iniciativas

Overview das principais iniciativas globais

Sovrin

Exemplo de uma plataforma que faz uso do framework Hyperledger Indy

Finalização

Comentários finais

Sovrin: camadas

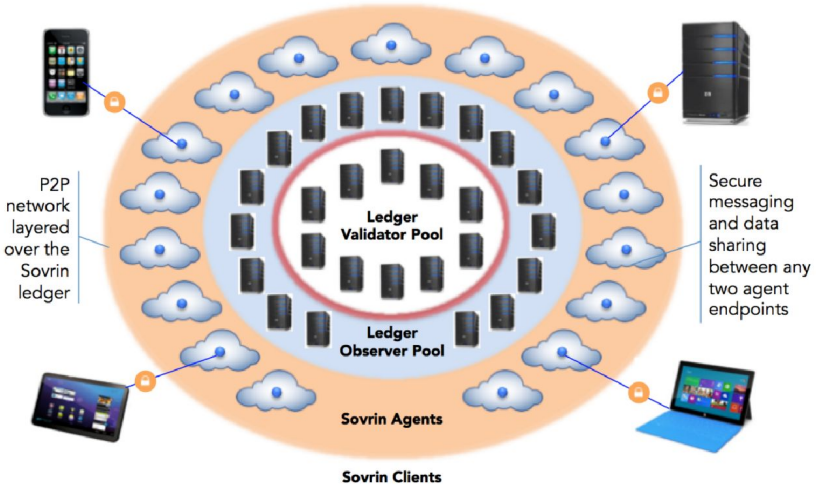
- **Sovrin Clientes:** são aplicações utilizadas pelos proprietários de identidades do Sovrin para comunicar com os agentes do Sovrin e com a ledger para realizar transações de identidade de todos os tipos.
- **Sovrin Agentes:** Os agentes Sovrin são um novo tipo de serviço de rede que proporciona aos proprietários de identidades da Sovrin uma forma permanente e protegida de realizar transações de identidade e gerenciamento de dados.
- **Sovrin Ledger:** ledger distribuída globalmente com registros de identidade raiz mantidos por instituições confiáveis em todo o mundo. Operada como uma utilidade pública global sem fins lucrativos.

Sovrin: Arquitetura

Tipos de nós:

- **Nós validadores**: executam o protocolo de consenso para validar novas transações do Sovrin. Cada gravação na ledger deve ser enviada para um nó validador. São chamados de Stewards;

- **Nós observadores**: serão necessários à medida que a rede crescer. Do ponto de vista dos clientes, um nó observador é simplesmente uma cópia somente leitura da ledger Sovrin. Trabalham em standy-by e podem assumir o papel de validadores.



Agenda

Exemplo de Plataforma: Sovrin

1. **ID**
   Contexto da Identidade Digital
2. **SSID**
   Identidade Digital Autossoberana
3. **Iniciativas**
   Overview das principais iniciativas globais
4. **Sovrin**
   Exemplo de uma plataforma que faz uso do framework Hyperledger Indy
5. **Finalização**
   Comentários finais

Comentários finais

- Comunidades de identidade autossoberanas continuam ganhando membros a cada dia
- Soluções e organizações voltadas para identidade autossoberana é um dos segmentos de mais rápido crescimento
- Poucas empresas conseguiram um produto de mercado e menos ainda acumularam uma massa crítica de usuários regulares
- Previsão de novos pilotos ainda esse ano, deve direcionar ainda mais o mercado